REMARKS

Claims 9, 11, 15, 17, 27, 29, 32, and 37-40 are pending in the instant application. Claims 9, 11, 15, 17, 27, 29, 32, and 37 presently stand rejected. Claims 9, 15, 27, and 37 are amended herein. Claims 38-40 are newly presented. Claim 32 is hereby cancelled without prejudice. Entry of this amendment and reconsideration of the pending claims are respectfully requested.

Claim Objections

Claim 9 stands objected to for failure to include a semicolon at the end of line 6. Claim 9 has been amended to cure this inadvertent error.

Claim Rejections – 35 U.S.C. § 103

Claims 9, 11, 15, 17, 32, and 37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine et al. (US 6,397,242), in view of "Extensible Firmware Interface Specification (Version 1.02, December 12, 2000), and in further view of Davis (US 5,844,986).

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. All words in a claim must be considered in judging the patentability of that claim against the prior art." M.P.E.P. § 2143.03.

Amended independent claim 9 now recites, in pertinent part,

> restricting access by the firmware modules to a subset of system resources provided by the native environment and to a subset of a memory map of the native environment, via the VMM; and
>
> **authenticating, via the VMM**, at least one of the firmware modules that is loaded during the pre-boot phase by comparing a digital signature provided with the at least one of the firmware modules with valid digital signatures stored in a secure storage that is **accessible to the VMM, but which the VMM makes inaccessible to the firmware modules and the legacy code.**

Applicants respectfully submit that the combination of Devine, the EFI Specification, and Davis fails to disclose, teach, or suggest using a VMM to authenticate firmware modules. Furthermore, the cited prior art fails to teach or suggest using the VMM to make valid digital signatures inaccessible to firmware modules running on a computer

system by rendering the secure storage inaccessible to the firmware modules and legacy code.

To be sure, the Examiner acknowledges that "Devine in view of Intel [the EFI Specification] does not explicitly disclose the limitations of authenticating firmware modules as recited by the claim [9]." *Office Action* mailed 11/02/05, page 6. However, the Examiner cites Davis as disclosing this missing element.

Davis in fact discloses the use of a cryptographic coprocessor 34, illustrated in FIG. 1, to authenticate BIOS programs 43. Cryptographic coprocessor 34 includes a bus interface 40 for coupling to system bus 33 and a processing unit 41. Cryptographic coprocessor 34 is a physical hardware element. Accordingly, Davis discloses use of a hardware cryptographic coprocessor 34 to perform authentication of firmware modules.

In contrast, independent claim 9 recites authenticating firmware modules with a VMM. A VMM is software—not hardware—and distinctly different from a cryptographic coprocessor. Additionally, independent claim 9 recites storing valid digital signatures in a secure storage that is **accessible to the VMM,** but which **the VMM makes inaccessible** to firmware modules and legacy code. Davis discloses a hardware cryptographic coprocessor 34 for protecting BIOS program 43. However, Davis does not teach or suggest using a VMM to safeguard valid digital signatures by storing the valid digital signature in a secure storage that a VMM makes inaccessible.

Consequently, the combination of Devine, the EFI Specification, and Davis fails to teach or suggest all elements of claim 9, as required under M.P.E.P. § 2143.03. Amended independent claims 15 and 27 include similar nonobvious elements as independent claim 9. Accordingly, Applicants request that the instant §103(a) rejections of claims 9, 15, and 27 be withdrawn.

The dependent claims are nonobvious over the prior art of record for at least the same reasons as discussed above in connection with their respective independent claims, in addition to adding further limitations of their own. Accordingly, Applicants respectfully request that the instant § 103 rejections of the dependent claims be withdrawn.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants believe the applicable rejections have been overcome and all claims remaining in the application are presently in condition for allowance. Accordingly, favorable consideration and a Notice of Allowance are earnestly solicited. The Examiner is invited to telephone the undersigned representative at (206) 292-8600 if the Examiner believes that an interview might be useful for any reason.

CHARGE DEPOSIT ACCOUNT

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a). Any fees required therefore are hereby authorized to be charged to Deposit Account No. 02-2666. Please credit any overpayment to the same deposit account.

Respectfully submitted,

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

Date: Jan. 27, 2006

Cory G. Claassen
Reg. No. 50,296
Phone: (206) 292-8600